UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,058	01/10/2002	Paul Harry Abbott	GB920010007US1	9940

46320 7590 08/16/2007

CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
08/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

AUG 16 2007

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/046,058
Filing Date: January 10, 2002
Appellant(s): ABBOTT, PAUL HARRY

Scott D. Paul
Reg. No. 42,984
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/1/2007 appealing from the Office action mailed 3/2/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2001/0008012	Kausik	12-2000
5,706,513	Bahls et al.	7-1995
7,003,109	Henson et al.	3-2001

"Hash Collision", Wikipedia.org <URL:http://en.wikipedia.org/wiki/Hash_collision>

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4-9, 11-14, 16-24, and 26-31, 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kausik United States Patent Application Publication No. 2001/0008012 (hereinafter "Kausik"), and Bahls et al U.S. Patent No. 5,706,513 (hereinafter "Bahls").

Kausik teaches storage of security keys and certificates in a storage means, but fails to explicitly teach fragmenting the keys or certificates. (Kausik Figure 1, paragraphs 11, 24-32)

However, in related art, Bahls discloses a system for the storage and fragmentation of files. (Bahls et al Col 5 lines 55-67 – Col 6 lines 1-3, figure 6).

As taught by Kausik (paragraph 27) the keys/certificates are stored in any standard storage medium including floppy disks, hard disks, magnetic stripe cards, and smart cards, such media as taught by Bahls is advantageously shared amongst several

applications. Wherein the working storage of a given application is not large enough to store an entire data object it is desirable to fragment such a data object into multiple pieces and store those pieces (Bahls Col 1 lines 55-67, Col 2 lines 2-20, Col 3 lines 35-40). Additionally, such fragments when for instance N=2 exists for a given object (key or certificate) and the size is not a multiple of the segment size will be of a non-uniform nature in length when stored and intermixed in the storage medium (Bahls Col 5 lines 55-67).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Bahls with those of Kausik in order to facilitate shared storage amongst applications wherein the working storage of those given applications is not adequate to store an entire working object.

Regarding Claims 1, 13, 23: storing a key or a certificate in a storage means (Kausik figure 1, paragraphs 24-32; Bahls figure 6, Col 5 lines 55-67, Col 3 lines 35-40) Kausik teaches storing keys encrypted with a pin in a key wallet.
Fragmenting the key or certificate into non-uniform lengths according to an algorithm (Bahls Col 5 lines 55-67, fig 6) Clearly as taught when a situation exists wherein N=2 and the object size is not a multiple of the segment size the key would be fragmented into pieces of non-uniform length and stored in the associated medium.
Fragments are intermixed with storage means (Bahls figure 7, Col 3 lines 5-17, Col 5 lines 55-67) As provided by the teachings of Bahls and seen in figure 7 the objects are stored amongst each other in shared storage and are therefore intermixed as claimed.

Regarding Claim 2: The storage means is a data file (Kausik paragraph 11, 27, figure 1) Kausik states that the implementation dictates a software implementation of storage of the keys, hence the key is clearly stored in a file on a tangible means.

Regarding Claim 4: Fragmenting the entity includes fragmenting the bytes (Bahls Col 5 lines 33-66) The division of any digital file has to be in such a manner as to be fragmenting the bytes, since the bytes are what the file is composed of, and the act of fragmenting an object consists of separating it amongst its smaller pieces.

Regarding Claim 5: Location of storing fragments is determined by the algorithm (Bahls Col 5 lines 33-67, Col 6 lines 1-3, figures 3, 8) As stated by Bahls the file is fragmented in relation to its storage location since the fragments are created as a purpose of the storage location and furthermore as provided for by the associated key which is stored with the object for recovery.

Regarding Claim 6: Algorithm can be used to find the fragments (Bahls Col 5 lines 33-67, Col 6 lines 1-3, figure 8) As stated previously an algorithm must be used to perform such a function and furthermore the implementation of such an algorithm provides for a reciprocal process. The provided key that is stored with the data objects provides for putting the file back together and relates each piece with the next through the fragments of the key.

Regarding Claim 7: Storage means has a pass code used by the algorithm (Kausik paragraph 24-26, 37) Kausik provides an encrypted key, that is encrypted by a PIN, that can only be decrypted by use of that same PIN.

Regarding Claim 8: Fragments stored at locations determined by pass code (Kausik paragraph 24-26, 37; Bahls Figure 8, Col 3 lines 45-65, Col 6 lines 1-41)

Regarding Claim 9: Bit map as a record of fragment locations (Bahls Fig 2, Fig 7) As it can be seen from the figures the Implementation of this system provides for a bit map as a record of fragment locations. During the processing of these files they are staged into queues and as such have formed a map of the actual file since it is no longer together but segmented into bits and thus only represented while staged. These segmented bit patterns provide for the reconstruction of the file upon it's use or the file being placed back into permanent storage.

Regarding Claim 11 and 12: the storage means is a keystore repository; the algorithm is implemented as a keystore class (Kausik paragraph 11, figure1; Bahls Col 5 lines 55-67, figure 7-8)

Claims 14, 16-24, 26-31, 33-34 are an apparatus and computer program product implementation of the above rejected claims and as such are rejected on the same basis.

and 32

Claims 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kausik United States Patent Application Publication No. 2001/0008012 (hereinafter "Kausik"), and Bahls et al U.S. Patent No. 5,706,513 (hereinafter "Bahls") as applied to claim 1 above.

Regarding Claim 10: Fragment stored immediately after another if storage location is occupied. It is well known within the art that when implementing an algorithm

such as a hash algorithm for the placement of objects amongst potential storage spots that when a collision occurs the object is stored immediately following the occupied spot. Thus Official notice is given that performing such an operation is a well known practice within the art.

Claim 32 is a computer program product implementation of the above rejected claim and as such is rejected on the same basis.

Claims 3, 15, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kausik United States Patent Application Publication No. 2001/0008012 (hereinafter "Kausik"), Bahls et al U.S. Patent No. 5,706,513 (hereinafter "Bahls") as applied to claim 1 above, and further in view of Henson et al United States Patent No. 7,003,108 (hereinafter "Henson").

The combination of Bahls and Kausik teaches a manner of storing keys and certificates as in claim 1 above and individually teach both the use of nulls (Bahls Col 5 lines 66-67) in storage and as in the case of Kausik random data padded onto a message (Kausik claim 22), but both fail to explicitly teach random bit patterns within the storage means.

However, in related art, Henson teaches the use of random characters for padding. Henson teaches that the use of random characters to pad encrypted data is advantageous since it provides for better concealing the encrypted data in storage (Henson Col 12 lines 1-9).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Henson with those of the above combination for a more secure system by better concealing the encrypted data as denoted by Henson.

Regarding Claim 3: Storage means contains random bit patterns (Henson Col 12 lines 1-9).

(10) Response to Argument

The appellant in forming a stance against the present rejection has cited to portions of Bahls, which state that it is not necessary to fragment a data object if the data object is smaller than the available storage capacity of the working storage. The examiner asserts, however, that at the time of the cited art of Bahls, circa 1995, storage in many devices especially those envisioned in this combination such as PDA devices and other small portable electronics contained very small memory that was shared between multiple applications. Bahls teaches that the working storage represents a finite amount of memory (Bahls Col 1 lines 24-25), which is shared between multiple applications. Bahls further recites that large data objects can render an application incapable of performing their functions and that any data object that is larger than the working storage is defined as a large data object for the purposes of the disclosure (Bahls Col 1 lines 36-47). At the time of this disclosure the working storage for such a device as a PDA was clearly within the range that segmentation of an object the length of a key or even more so a certificate, which is generally many times larger than a key

since a certificate often contains a key and other information such as a message digest, when shared with other applications would have required being split up as set forth by the current combination and thus then would be a viable and reasonable combination.

The appellant's example of a system wherein the storage capacity is 40 gigabytes is an extremely narrow example of one embodiment and within such a case something such as a key may not be fragmented depending upon the size of the working storage, which Bahls states is of a variable size and not generally understood as being a hard drive, which is so large, but rather memory which is much more limited (Bahls Col 3 lines 24-25). Additionally, the intended embodiment of a device such as a PDA sets forth an embodiment which clearly would require segmentation and does not have vast amounts of storage capacity as cited by the appellant especially circa 1995, which is the time of the disclosure of Bahls. Therefore, when taking into consideration the state of devices present at the time of the disclosure of Bahls and the limited amount of memory available to those devices especially in the context of a PDA or other small portable device one of ordinary skill in the art would have been motivated to make such a combination and such a combination clearly would provide for splitting a key or certificate as disclosed by the appellant since the size of storage in these devices would have been very limited.

The recitation of a key being stored with the data object does not necessitate that the key is of the same size as the data object key, which is being split up, but as can be appreciated by one skilled in the art such a key is clearly capable of only being a few

bits and can thus easily be stored with the split portions of the data object key or certificate.

The algorithm which determines the manner of splitting the data object of Bahls splits the object based upon the size of the storage space, therefore the algorithm inherently determines the storage location when splitting the object since it does so based upon the size of that location, thus providing for The Algorithm performing both functions (Bahls Col 3 lines 24-25).

The limitations of claim 10 as previously stated are old and well known within the art. The limitations are so well known that the disclosure of Bahls would not be concerned with explaining such a practice since one of ordinary skill would assume that any system of this nature performs those basic steps. The argument is not that it is obvious to try as set forth by the appellant but rather that this is an intrinsic part of any such system.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Thomas M. Szymanski 8-10-07

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Conferees:

Kambiz Zand

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Kim Vu